DESCRIPTION

METHOD AND SYSTEM FOR PROXY-BASED SECURE END-TO-END TCP/IP COMMUNICATIONS

TECHNICAL FIELD

The present invention relates to a communication system using TCP/IP protocols. The present invention also relates to (a) a server apparatus for use in communication by pier to pier connection between equipments connected to a network such as the Internet or the like; (b) a request issuance equipment that issues a connection request signal; (c) a request acceptance equipment that accepts a connection request signal; (d) a server apparatus; (e) a communication system including the request issuance equipment and the request acceptance equipment; and (f) a communication method. The present invention further relates to a program including steps in the communication method.

BACKGROUND ART

In recent years, since broadband environments for xDSL, optical fiber cable, or the like have been constructed, the Internet has been increasingly spread not only in companies but also in ordinary household. In addition, not only (a) a personal computer (PC) but also (b) an AV apparatus such as a television receiver or a DVD recorder, (c) an air conditioner, and (d) a household electric apparatus such as a refrigerator can be connected to the Internet. In the present specification, an apparatus connected to the network such as the Internet and communicating with the other equipment will be referred to as "communication equipment" or "equipment".

In order to connect a local area network (referred to as a LAN

hereinafter) in a house or a company to the Internet, a router apparatus that has a network address translation (referred to as a NAT hereinafter) function and a network address port translation (referred to as a NAPT hereinafter) function is normally employed.

When a communication is executed between equipments connected to the Internet, a global IP address uniquely allocated to each equipment is used. However, the number of global IP addresses tends to decrease because of rapid increase in the number of equipments connected to the Internet. This leads to that a private IP address that is unique only in a LAN specified according to RFC1918 is often used in a LAN that is not directly connected to the Internet. It is noted that the private IP address is not unique on the Internet and is not permitted to be used on the Internet. This leads to that the equipment having the private IP address cannot communicate with the other equipment connected to the Internet without any support for the equipment.

The NAT function or the NAPT function solves this problem. The NAT or NAPT function executes translation between the private IP address and the global IP address, so that the equipment to which the private IP address is allocated and which is connected to the LAN can communicate with the other equipment connected to the Internet.

A mechanism of the NAPT function will be described with reference to Figs. 10 to 12.

Fig. 10 is a block diagram showing one example of a network configuration of a prior art communication system. Referring to Fig. 10, a request acceptance equipment 13 and a router apparatus 104 having

the NAPT function constitute a LAN 106, and the LAN 106 is connected to the Internet (WAN) 105 at a WAN side port of the router apparatus 104. The server apparatus 11 and the request issuance equipment 12 are also connected to the Internet (WAN) 105.

In order to distinguish the so-called Internet from the LAN, the Internet will be denoted herein by WAN (Wide Area Network).

Fig. 11 shows one example of a communication sequence diagram for a communication using the NAPT function. Referring to Fig. 11, a packet 21 is transmitted from the request acceptance equipment 13 to the router apparatus 104. A packet 23 is transmitted from the router apparatus 104 to the server apparatus 11 by allowing the router apparatus 104 to execute a step 22 of a forward path conversion processing on the packet 21. Further, a packet 25 is transmitted from the server apparatus 11 to the router apparatus 104. A packet 27 is transmitted from the router apparatus 104 to the request acceptance equipment 13 by allowing the router apparatus 104 to execute a step S26 of a backward path conversion processing on the packet 25. Furthermore, Fig. 12 is a table showing one example of a NAPT table of the router apparatus 104. The contents of this NAPT table are stored in a table memory (not shown) included in the router apparatus 104.

As shown in Fig. 10, it is assumed that a global IP address of "130.74.23.6" is allocated to the server apparatus 11, a global IP address of "202.204.16.13" is allocated to a WAN side of the router apparatus 104, and that a private IP address of "192.168.1.3" is allocated to the request acceptance equipment 13.

An IP packet for use in a communication on the Internet includes a source IP address field (referred to as an SA hereinafter) that specifies a source, and a destination IP address field (referred to as a DA hereinafter) that designates a destination. In addition, when a TCP (Transmission Control Protocol) or a UDP (User Datagram Protocol) is used as a communication protocol, the IP packet also includes a source port number field (referred to as an SP hereinafter) that is a port number of the source, and a destination port number field (referred to as a DP hereinafter) that is a port number of the destination.

When the request acceptance equipment 13 executes a TCP communication with the server apparatus 11, the request acceptance equipment 13 transmits the packet 21 shown in Fig. 11, for example, to the router apparatus 104. The packet 21 includes an SA of "192.168.1.3" and an SP of "2000" that specify a source, and a DA of "130.743.23.6" and a DP of "1200" that specify a destination.

The router apparatus 104 executes the forwarding path conversion processing on the received packet 21 at step S22, and transmits the processed packet 23 to the server apparatus 11 that is the destination of the packet. At the forward path conversion processing of the step S22, the router apparatus 104 replaces the SA of "192.168.1.3" that is the private IP address by "202.204.16.13" that is a global IP address of the WAN side of the router apparatus 104. In addition, the router apparatus 104 replaces the SP of "2000" by a WAN side port number of "3400" of the router apparatus 14. At this time, the router apparatus 104 stores a set of the IP addresses of "192.168.1.3"

and "202.204.16.13" and the port numbers of "2000" and "3400" in the NAPT table, as shown in Fig. 12.

When receiving the packet 23, the server apparatus 11 executes a predetermined response processing at step S24, and thereafter, transmits the packet 25 to the router apparatus 104 as a response to the packet 23. The packet 25 includes an SA of "130.743.23.6" and an SP of "1200" that specify a source, and a DA of "202.204.16.13" and a DP of "3400" that specify a destination.

When receiving the packet 25, the router apparatus 104 makes reference to the NAPT table, executes the backward path conversion processing on the packet 25 at step S26, and transmits the processed packet 27 to the request acceptance equipment 13. At the backward path conversion processing of the step S26, the router apparatus 104 first of all makes reference to the pair of the DA of "202.204.16.13" and the DP of "3400" in the NAPT table. Since this pair is present therein, the router apparatus 104 replaces the DA of "202.204.16.13" of the packet 25 by the DA of "192.168.1.3", and then, replaces the DP of "3400" of the packet 25 by the DP of "2000".

The data stored in the NAPT table is held during the communication, and is abandoned after the end of the communication.

Through this operation, the equipment that has the private IP address on the LAN can communication with the other equipment connected to the Internet. However, conversely, the equipment connected to the Internet cannot start communicating with the equipment having the private IP address on the LAN.

In order to solve this problem, a function as called "static NAPT" is provided. In other words, a static NAPT table is set on the router apparatus 104 in advance. The contents of the static NAPT table are equal to those of the NAPT table shown in Fig. 12. However, in this case, an unused port number should be designated as a WAN side port number during a setting. Use of the static NAPT function has the following advantageous effect. For example, when the Internet-side equipment transmits a packet to the router apparatus 104 with a set global IP address and a set port number, the router apparatus 104 translates the IP address and the port number in a manner similar to that of the operation shown in Fig. 11. Then the packet arrives at the request acceptance equipment 13 having the private IP address and being connected to the LAN. As a result, the equipment connected to the Internet can communicate with the equipment having the private IP address on the LAN.

By the way, the global IP address of the router apparatus 104 is not always fixed. For example, when the router apparatus 104 is connected to an Internet service provider using a PPP (Point-to-Point protocol) or an IP address is dynamically allocated to the router apparatus 104 according to a DHCP (Dynamic Host Configuration Protocol), the global IP address often changes whenever the router apparatus 104 is connected to the Internet. This makes it difficult to grasp the global IP address of the equipment to be connected. In addition, if the static NAPT is used, the equipment can access to the other equipment on the LAN even while no communication is being

executed therebetween, and this leads to that security is disadvantageously reduced.

In order to solve these problems, a communication system is proposed in the International Publication WO-2004-030314-A1 which is a family of the Japanese Patent No. 3,445,986. The communication system proposed in the same International Publication will be described with reference to Figs. 10 to 13.

Fig. 13 is a sequence diagram of one example of a communication sequence for the communication system shown in Fig. 10. As shown in Fig. 10, it is assumed that a global IP address of "8.117.12.109" is allocated to the request issuance equipment 12. It is also assumed that the request acceptance equipment 13 stores an equipment ID uniquely allocated to the equipment 13 in the internal memory (not shown) thereof.

The request acceptance equipment 13 periodically transmits an equipment registration packet 31 that includes the equipment ID in a payload to the server apparatus 11 using the UDP. In an SA of the equipment registration packet 31 that is a UDP packet, "192.168.1.3" that is the private IP address of the request acceptance equipment 13 is written. When the equipment registration packet 31 passes through the router apparatus 104, an SA and an SP of the equipment registration packet 31 are translated by the NAPT function as described above, and the translated packet 31 is transmitted to the server apparatus 11. The server apparatus 11 makes reference to the received equipment registration packet 31, and stores a set of the equipment ID, a global IP

address, and a port number of the request acceptance equipment 13 at step S32.

The request acceptance equipment 13 periodically transmits the equipment registration packet 31 to the server apparatus 11. Therefore, even if the global IP address or the WAN side port number of the router apparatus 104 is changed, the equipment ID, a set of the global IP address, and the port number of the request acceptance equipment 13 stored in the server apparatus 11 are automatically updated by executing the step S32, a step S32A similar to the step S32, or the like.

On the other hand, when the request issuance equipment 12 wishes to communicate with the request acceptance equipment 13, the request issuance equipment 12 first of all transmits a TCP connection start packet 33 to the server apparatus 11 to thereby establish a TCP connection with the server apparatus 11, and transmits a connection request packet 34 having the equipment ID of the request acceptance equipment 13, which is a connection counterpart, to the server apparatus 11. When receiving the connection request packet 34, the server apparatus 11 makes reference to an equipment ID list stored in the internal memory (not shown) at step S35. If information on the same equipment ID as the equipment ID included in the connection request packet 34 is present, the server apparatus 11 transmits a connection request notification packet 36 to the equipment indicated by the IP address and the port number as associated with this equipment ID using the UDP. The connection request notification packet 36 is transmitted to the router apparatus 104 as a response to the equipment

registration packet 31. Therefore, the IP address and the port number are translated by the router apparatus 104, so that the connection request notification packet 36 can arrive at the request acceptance equipment 13. When receiving the connection request notification packet 36, the request acceptance equipment 13 transmits a TCP connection start packet 37 to the server apparatus 11, then establishing a TCP connection with the server apparatus 11.

Thereafter, when the request issuance equipment 12 transmits a command signal 38 to the server apparatus 11 using the TCP connection started by the TCP connection start packet 33, the server apparatus 11 can transfer the command signal 38 to the request acceptance equipment 13 using the TCP connection started by the TCP connection start packet 37. Further, when the request acceptance equipment 13 transmits the packet to the server apparatus 11 using the TCP connection started by the TCP connection start packet 37, the server apparatus 11 can transfer this packet to the request issuance equipment 12 using the TCP connection started by the TCP connection start packet 33.

In this way, the relay of the server apparatus 11 can execute the communication between the request issuance equipment 12 that is the equipment having the global IP address and connected to the Internet and the request acceptance equipment 13 that is the equipment having the private IP address and connected to the LAN. Even if the request issuance equipment 12 is present in the other LAN and is connected to the Internet through the router apparatus, the request issuance

equipment 12 can communicate with the request acceptance equipment 13 by the same operation.

Furthermore, the Japanese Patent Application Laid-Open Publication No. 2003-203023 discloses an information processing system for directly transmitting global IP addresses between unknown equipments connected to the Internet, that is, for performing pier to pier transmission. Personal computers that are clients each having a global ID address are connected to each other by pier to pier connection, whereas the other clients are connected to each other by client-server connection via a server. The pier to pier connection is established based on the mutual global IP addresses acquired from the server. By partially changing the client-to-server connection to the pier to pier connection, a local concentration of traffic on the server can be prevented.

However, the communication system disclosed in the International Publication WO-2004-030314-A1 has the following problems. The communication system disclosed in the same International Publication always executes a communication via the server apparatus 11. Due to this, when a larger capacity of data such as moving image data is transmitted between the equipments, a larger load is applied to the server apparatus. In particular when a plurality of communications is executed at the same time, the communications cannot be sometimes dealt with even by a distributed processing using a plurality of server apparatuses.

Furthermore, the information processing system disclosed in the

Japanese Patent Application Laid-open Publication No. 2003-203023 performs the pier to pier transmission only between the equipments having the global IP addresses and not between the equipments having the private IP addresses and connected to the LAN.

DISCLOSURE OF THE INVENITON

It is an object of the present invention to provide a server apparatus, a request issuance equipment, a request acceptance equipment, a communication system, and a communication method capable of solving the above-mentioned problems of the prior art, realizing a pier to pier communication between equipments each having a private IP address but located on different LANs with prohibiting any illegal access.

It is another object of the present invention to provide a program including steps in the communication method.

According to a first aspect of the present invention, there is provided a server apparatus provided in a communication system. In the communication system, the server apparatus and a plurality of equipment including a request issuance equipment and a request acceptance equipment are each connected to a network, and the server apparatus being operable to transfer a connection request signal from the request issuance equipment to the request acceptance equipment. The server apparatus includes an equipment information storage device operable to store an equipment information list that includes a set of equipment information for each of the plurality of equipment, where the set of equipment information included an IP address and a port number

as associated with each of the plurality of equipment, and an equipment ID of each of the plurality of equipment.

The server apparatus is operable to receive an equipment registration signal which includes a set of equipment information for the request acceptance equipment, and which is periodically transmitted from the request acceptance equipment, and is operable to store a set of equipment information for the request acceptance equipment included in the received equipment registration signal in the equipment information storage device. The server apparatus is operable to receive a first TCP connection start signal transmitted from the request issuance equipment for establishing a first TCP connection with the request issuance equipment. The server apparatus is operable to receive a first connection request signal which includes the equipment ID of the request acceptance equipment, and the IP address and the port number as associated with the request issuance equipment, and which is a request to the request acceptance equipment, from the request issuance equipment using the first TCP connection. The server apparatus is operable to search the equipment ID of the request acceptance equipment included in the received first connection request signal from the equipment information list, identify the equipment related to a set of equipment information that includes the equipment ID coincident with the equipment ID of the request acceptance equipment included in the first connection request signal as the request acceptance equipment, and identify the IP address and the port number included in a set of equipment information for the identified request

acceptance equipment as the IP address and the port number as associated with the request acceptance equipment on the equipment information list. The server apparatus is operable to transmit a second connection request signal that includes the IP address and the port number included in the received first connection request signal and associated with the request issuance equipment to the identified request acceptance equipment, as a response signal to the equipment registration signal, with the identified IP address and the identified port address set as a destination.

In the above-mentioned server apparatus, after identifying the IP address and the port number included in a set of equipment information for the identified request acceptance equipment as the IP address and the port number as associated with the request acceptance equipment, and before transmitting the second connection request signal to the identified request acceptance equipment, the server apparatus transmits a third connection request signal to the request acceptance equipment, and receives a second TCP connection start signal from the request acceptance equipment as a response signal to the third connection request signal to establish a second TCP connection with the request acceptance equipment. The server apparatus is operable to transmit the second connection request signal to the request acceptance equipment using the established second TCP connection.

In the above-mentioned server apparatus, the first connection request signal further includes password information for the request

acceptance equipment. The server apparatus is operable to add the password information included in the first connection request signal to the second connection request signal, and transmit the second connection request signal including the password information.

The above-mentioned server apparatus further includes a first encryption communication device, and a certificate information storage device. The first encryption communication device is operable to generate a first common key for communication and a second common key for communication, to decrypt the received signal using the first common key for communication, and to encrypt the transmitted signal using the second common key for communication. The certificate information storage device is operable to store server certificate information for certifying a validity of the server apparatus.

The server apparatus is operable to transmit the server certificate information to the request issuance equipment before receiving the first connection request signal. The server apparatus is operable to receive first common key generation information generated in response to the server certificate information from the request issuance equipment using the first TCP connection, cause the first encryption communication device to generate second common key generation information in response to the first common key generation information, cause the first encryption communication device to generate the first common key for communication based on the first common key generation information and the second common key generation information, transmit the second common key generation information to

the request issuance equipment using the first TCP connection, and cause the request issuance equipment to generate a common key for communication identical with the first common key for communication based on the first common key generation information and the second common key generation information to share the first common key for communication with the request issuance equipment. The server apparatus is operable to receive the first connection request signal encrypted using the first common key for communication, from the request issuance equipment using the first TCP connection, and cause the first encryption communication device to decrypt the received first connection request signal using the first common key for communication. Before transmitting the second connection request signal, the server apparatus transmits the server certificate information to the request acceptance equipment. The server apparatus is operable to receive third common key generation information generated in response to the server certificate information from the request acceptance equipment using the second TCP connection, cause the first encryption communication device to generate fourth common key generation information in response to the third common key generation information, causes the first encryption communication means to generate the second common key for communication based on the third common key generation information and the fourth common key generation information, transmit the fourth common key generation information to the request acceptance equipment using the second TCP connection, and cause the request acceptance equipment to generate a

common key for communication identical with the second common key for communication based on the third common key generation information and the fourth common key generation information to share the second common key for communication with the request acceptance equipment. After receiving the first connection request signal and before transmitting the second connection request signal, the server apparatus causes the first encryption communication device to encrypt the second connection request signal using the second common key for communication.

According to a second aspect of the present invention, there is a request issuance equipment provided in a communication system. In the request issuance equipment, a server apparatus and a plurality of equipment including the request issuance equipment and a request acceptance equipment are each connected to a network, and the request issuance equipment is operable to communicate with the server apparatus and the request acceptance equipment. The request issuance equipment is operable to transmit a first TCP connection start signal to the server apparatus for establishing a first TCP connection with the server apparatus. The request issuance equipment is operable to transmit a first connection request signal which includes an equipment ID of the request acceptance equipment, and an IP address and a port number as associated with the request issuance equipment, and which is a request to the request acceptance equipment, to the server apparatus using the first TCP connection. After receiving a communication request signal for requesting a communication between

the request issuance equipment and the request acceptance equipment from the request acceptance equipment, the request issuance equipment accepts the communication between the request issuance equipment and the request acceptance equipment in response to the communication request signal, and starts the communication with the request acceptance equipment.

In the above-mentioned request issuance equipment, the first connection request signal further includes password information for the request acceptance equipment.

The above-mentioned request issuance equipment further includes a second encryption communication device, and a first certificate information authentication device. The second encryption communication device is operable to generate a first common key for communication, and to encrypt the transmitted signal using the first common key for communication. The first certificate information authentication device is operable to authenticate server certificate information for certifying a validity of the server apparatus. The request issuance equipment is operable to receive the server certificate information from the server apparatus before transmitting the first connection request signal. The request issuance equipment is operable to authenticate the received server certificate information by the first certificate information authentication device and confirm whether or not the received server certificate information is valid. When confirming that the received server certificate information is valid, the request issuance equipment causes the second encryption communication

device to generate first common key generation information, transmit the generated first common key generation information to the server apparatus using the first TCP connection, receive second common key generation information generated in response to the first common key generation information from the server apparatus using the first TCP connection, cause the second encryption communication device to generate the first common key for communication based on the first common key generation information and the second common key generation information, and cause the server apparatus to generate a common key for communication identical with the first common key for communication based on the first common key generation information and the second common key generation information to share the first common key for communication with the server apparatus. Before transmitting the first connection request signal, the request issuance equipment causes the second encryption communication device to encrypt the first connection request signal using the first common key for communication. The request issuance equipment is operable to transmit the encrypted first connection request signal to the server apparatus using the first TCP connection.

According to a third aspect of the present invention, there is provided a request acceptance equipment provided in a communication system. In the communication system, a server apparatus and a plurality of equipment including a request issuance equipment and the request acceptance equipment are each connected to a network, the request acceptance equipment being operable to communicate with the

server apparatus and the request issuance equipment. The request acceptance equipment includes an equipment ID storage device operable to store an equipment ID of the request acceptance equipment. The request acceptance equipment is operable to periodically transmit an equipment registration signal which includes the equipment ID of the request acceptance equipment to the server apparatus. The request acceptance equipment is operable to receive a second connection request signal that includes an IP address and a port number as associated with the request issuance equipment from the server apparatus as a response signal to the equipment registration signal. The request acceptance equipment is operable to transmit a communication request signal for requesting a communication between the request acceptance equipment and the request issuance equipment to the request issuance equipment represented by the IP address and the port number included in the received second connection request signal. After the request issuance equipment accepts the communication between the request acceptance equipment and the request issuance equipment in response to the communication request signal, the request acceptance equipment starts the communication with the request issuance equipment.

In the above-mentioned request acceptance equipment, after transmitting the equipment registration signal to the server apparatus and before receiving the second connection request signal, the request acceptance equipment receives a third connection request signal from the server apparatus as a response signal to the equipment registration

signal, and transmits a second TCP connection start signal to the server apparatus as a response signal to the third connection request signal to establish a second TCP connection with the server apparatus. The request acceptance equipment is operable to receive the second connection request signal from the server apparatus using the established second TCP connection.

The above-mentioned request acceptance equipment further includes a password information storage device operable to store password information for the request acceptance equipment. The request acceptance equipment is operable to receive the second connection request signal that further includes password information from the server apparatus using the second TCP connection. The request acceptance equipment is operable to transmit the communication request signal to the request issuance equipment only when the password information included in the second connection request signal coincides with the password information for the request acceptance equipment stored in the password information storage device.

The above-mentioned request acceptance equipment further includes a third encryption communication device, and a second certificate information authentication device. The third encryption communication device is operable to generate a second common key for communication, and decrypt the received signal using the second common key for communication. The second certificate information authentication device is operable to authenticate server certificate

information for certifying a validity of the server apparatus. Before, receiving the second connection request signal, the request acceptance equipment receives the sever certificate information from the server apparatus. The request acceptance equipment is operable to cause the second certificate information authentication device to authenticate whether or not the received server certificate information is valid to confirm whether or not the received server certificate information is valid. When confirming that the received server certificate information is valid, the request acceptance equipment causes the third encryption communication device to generate third common key generation information, transmit the generated third common key generation information to server apparatus using the second TCP connection, receive fourth common key generation information generated in response to the third common key generation information from the server apparatus using the second TCP connection, cause the third encryption communication device to generate the second common key for communication based on the second common key generation information and the fourth common key generation information, and cause the server apparatus to generate a common key for communication identical with the second common key for communication based on the third common key generation information and the fourth common key generation information to share the second common key for communication with the server apparatus. The request acceptance equipment is operable to receive the second connection request signal encrypted using the second common key for

communication from the server apparatus using the second TCP connection, and cause the third encryption communication device to decrypt the received second connection request signal using the second common key for communication.

According to a fourth aspect of the present invention, there is provided a communication system including the server apparatus, a plurality of equipments including the request issuance equipment and the request acceptance equipment. In the communication system, the plurality of equipments and the server apparatus are each connected to the network.

According to a fifth aspect of the present invention, there is provided a communication method including steps which are executed by the server apparatus, the request issuance equipment and the request acceptance equipment.

According to a sixth aspect of the present invention, there is provided a program for causing a computer to perform the communication method.

Accordingly, according to the present invention, there can be realized a pier to pier communication between the request issuance equipment and the request acceptance equipment which are equipments each having a private IP address but located on different LANs with prohibiting any illegal access. Further, according to the present invention, the program can be provided including the steps in the communication method for allowing a computer or an equipment connected to the Internet to execute the steps in the communication

method when the program is read out by the computer or the equipment.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram of a network configuration of a communication system according to a preferred embodiment of the present invention;

Fig. 2 is a sequence diagram showing one example of a communication sequence executed in the communication system shown in Fig. 1;

Fig. 3 is a sequence diagram showing detailed processings at a first connection request sequence of step S203 shown in Fig. 2;

Fig. 4 is a sequence diagram showing detailed processings at a second connection request sequence of step S206 shown in Fig. 2;

Fig. 5 is a block diagram of a certificate authority apparatus 51 that authenticates whether or not a server apparatus 101 is valid for a request issuance equipment 102 and a request acceptance equipment 103 shown in Fig. 1;

Fig. 6 is a table showing one example of a NAPT table stored in an internal table memory 104am of a router apparatus 104a shown in Fig. 1;

Fig. 7A is a schematic diagram showing a configuration of a LAN side equipment registration packet 201 shown in Fig. 2;

Fig. 7B is a schematic diagram showing a configuration of a WAN side equipment registration packet 201 shown in Fig. 2;

Fig. 7C is a schematic diagram showing a configuration of a LAN

side connection request packet 217 shown in Fig. 3;

Fig. 7D is a schematic diagram showing a configuration of a WAN side connection request packet 217 shown in Fig. 3;

Fig. 8A is a schematic diagram showing a configuration of a LAN side connection request notification packet 205 shown in Fig. 2;

Fig. 8B is a schematic diagram showing a configuration of a WAN side connection request notification packet 205 shown in Fig. 2;

Fig. 8C is a schematic diagram showing a configuration of a LAN side connection request packet 226 shown in Fig. 4;

Fig. 8D is a schematic diagram showing a configuration of a WAN side connection request packet 226 shown in Fig. 4;

Fig. 9 is a table showing one example of an equipment information list stored in a table memory 101m of the server apparatus 101 shown in Fig. 1;

Fig. 10 is a block diagram showing one example of a network configuration of a prior art communication system;

Fig. 11 is a sequence diagram showing one example of a communication sequence for a communication using a NAPT function of a router apparatus;

Fig. 12 is a table showing one example of a NAPT table of the router apparatus 104; and

Fig. 13 is a sequence diagram showing one example of a communication sequence of the communication system shown in Fig. 10.

BEST MODE FOR CARRYING OUT THE INVENTION

Preferred embodiments of the present invention will be described hereinafter with reference to Figs. 1 to 9.

Fig. 1 is a block diagram showing one example of a network configuration of a communication system according to the preferred embodiment of the present invention. A request issuance equipment 102 and a router apparatus 104a having a NAPT function constitutes a request-issuance-side LAN 106a. The request-issuance-side LAN 106a is connected to the Internet (WAN) 105 at a WAN side port of the router apparatus 104a. Further, a request acceptance equipment 103 and a router apparatus 104b having a NAPT function constitutes a request-acceptance-side LAN 106b. The request-acceptance-side LAN 106b is connected to the Internet (WAN) 105 at a WAN side port of the router apparatus 104b. In addition, a server apparatus 101 is connected to the Internet (WAN) 105.

The communication system according to the present preferred embodiment includes a plurality of equipments, such as the request issuance equipment 102 and the request acceptance equipment 103, each connected to the Internet (WAN) 105, and the server apparatus 101 connected to the Internet (WAN) 105. In the communication system, the request issuance equipment 102 on the request-issuance-side LAN 106a transfers a connection request signal to the request acceptance equipment 103 on the request-acceptance-side LAN 106b through the server apparatus 101, and a communication is executed between the request issuance equipment 102 and the request acceptance equipment 103. In this communication system, the server

apparatus 101 includes a table memory 101m of an equipment information storage means or device that stores an equipment information list, shown in Fig. 9, including a set of equipment information on each equipment consisting of an IP address and a port number as associated with each equipment as well as an equipment ID of the equipment. The request acceptance equipment 103 periodically transmits an equipment registration packet 201 including a set of equipment information on the request acceptance equipment 103 to the server apparatus 101. The server apparatus 101 receives the equipment registration packet 201, and stores a set of equipment information on the request acceptance equipment 103 included in this received equipment registration packet 201 in the table memory 101m of the equipment information storage means at steps S202 and S202A shown in Fig. 2. The request issuance equipment 102 first of all executes a first connection request sequence of the step S203 when communicating with the request acceptance equipment 103. At step S203, the request issuance equipment 102 transmits a TCP connection start packet 211 to the server apparatus 101 to thereby establish a first TCP connection with the server apparatus 101, and then, transmits a connection request packet 217 which includes the equipment ID of the request acceptance equipment 103, and the IP address and the port number as associated with the request issuance equipment 102, which is to be transmitted to the request acceptance equipment 103, to the server apparatus 101 using the first TCP connection. The server apparatus 101 receives the connection request packet 217. At step

S204, the server apparatus 101 searches the equipment ID of the request acceptance equipment 103 included in the received connection request packet 217 from the equipment information list, identifies the equipment related to a set of equipment information including an equipment ID coincident with the equipment ID of the request acceptance equipment 103 included in the connection request packet 217 as the request acceptance equipment 103 on the equipment information list, and identifies the IP address and the port number included in a set of equipment information as associated with the identified request acceptance equipment 103 as the IP address and the port number as associated with the request acceptance equipment 103 on the equipment information list. At step S205, the server apparatus 101 transmits a connection request packet 226 including the IP address and the port number as associated with the request issuance equipment 102 and included in the received connection request packet 217 to the identified request acceptance equipment 103 as a response signal to the equipment registration packet 201, with the identified IP address and port number used as a destination. The request acceptance equipment 103 receives the connection request packet 226. In addition, the request acceptance equipment 103 transmits a TCP connection request packet 208 to the request issuance equipment 102 represented by the IP address and the port number included in the received connection request packet 226, as a communication request signal for requesting a communication between the request issuance equipment 102 and the request acceptance equipment 103. When the

request issuance equipment 102 accepts the communication between the request issuance equipment 102 and the request acceptance equipment 103 in response to the TCP connection request packet 208, a data communication sequence for data communication between the request issuance equipment 102 and the request acceptance equipment 103 is started at step S209.

In the present preferred embodiment, the server apparatus 101, the request issuance equipment 102, and the request acceptance equipment 103 may be constituted as a dedicated communication equipment or a general-purpose computer operating by a computer readable program for executing a plurality of steps which will be described later.

In the present preferred embodiment, it is assumed as follows, as shown in Fig. 1. "130.74.23.6" is allocated as a global IP address to the server apparatus 101, which includes the table memory 101m that stores its global IP address and the equipment information list. "192.168.1.11" is allocated as a private IP address to the request issuance equipment 102. "192.168.1.3" is allocated as a private IP address to the request acceptance equipment 103. The request issuance equipment 102 includes a table memory 102m that stores its private IP address and port number. The request acceptance equipment 103 includes a table memory 103m that stores its private IP address and port number. "4.17.168.2" is allocated as a global IP address to the router apparatus 104a, and "202.204.16.13" is allocated as a global IP address to the router apparatus 104b. The router

apparatus 104a stores the contents of the NAPT table of Fig. 6 in an internal table memory 104am thereof, in a manner similar to that shown in Fig. 12, including its WAN side port number and global IP address, and the private IP address and port number of the request issuance equipment 102. Further, the router apparatus 104b stores the contents of a NAPT table including its WAN side port number and global IP address, and the private IP address and port number of the request acceptance equipment 103, in an internal table memory 104bm.

It is also assumed as follows. The request issuance equipment 102 stores an equipment ID of "1051" uniquely allocated to the equipment 102 in the internal table memory 102m thereof, and the request acceptance equipment 103 stores an equipment ID of "2133" uniquely allocated to the equipment 103 in the internal table memory 103m thereof. The equipment ID is identification information uniquely specified to each equipment of the present preferred embodiment that executes a pier to pier communication. For example, an identification number allocated by a manufacturer of the equipment or a MAC address can be used as the equipment ID. However, the equipment ID is not limited to them.

It is further assumed that the request acceptance equipment 103 stores a password that is secret information in the internal table memory 103m thereof. As will be described later, the request issuance equipment 102 that executes a pier to pier communication with the request acceptance equipment 103 needs to acquire a password and the equipment ID of the request acceptance equipment 102, and the global

IP address and the WAN side port number of the router apparatus 104a in advance, and to store them in the internal table memory 102m thereof.

Figs. 2 to 4 are sequence diagrams showing one example of communication sequences which is executed in the communication system shown in Fig. 1. Figs. 7A to 7D and Figs. 8A to 8D show examples of a plurality of packets for use in the communication sequences shown in Figs. 2 to 4.

The request acceptance equipment 103 transmits the equipment registration packet 201 having the equipment ID included in a payload to the server apparatus 101 using the UDP either periodically or at predetermined cycle intervals. As shown in Fig. 7A, on the request-acceptance-side-LAN 106b, "192.168.1.3" is written to an SA of the equipment registration packet 201, and "2000" is written to an SP of the equipment registration packet 201. The equipment registration packet 201 is transmitted to the server apparatus 101 through the router apparatus 104b. When the equipment registration packet 201 passes through the router apparatus 104b, the router apparatus 104b translates the SA on the equipment registration packet 201 to "202.204.16.13", and also translates the SP on the equipment registration packet 201 to "3400" by the NAPT function. The equipment registration packet 201 translated by the NAPT function, shown in Fig. 7B, is transmitted to the server apparatus 101 via the Internet (WAN) 105.

The server apparatus 101 includes the table memory 101m that

stores the equipment information list including a set of equipment information on respective equipments connected to the Internet (WAN) 105 and consisting of the IP address and the port number as associated with each equipment and the equipment ID of each equipment. The server apparatus 101 makes reference to the SA, the SP, and the payload of the received equipment registration packet 201, and then, at step S202, the server apparatus 101 stores a set of the equipment ID of the request acceptance equipment 103, the global IP address of the router apparatus 104b, and the WAN side port number of the router apparatus 104b in the table memory 101m included in the server apparatus 101 as a set of equipment information (that is, items of the equipment information list) corresponding to the request acceptance equipment 103. In the present preferred embodiment, the server apparatus 101 makes reference to the global IP address and the WAN side port number of the router apparatus 104b as the IP address and the port number as associated with the request acceptance equipment 103. In other words, when the server apparatus 101 transmits a packet to the request acceptance equipment 103, the server apparatus 101 makes reference to the global IP address and the WAN side port number of the request-acceptance-side LAN 106b including the request acceptance equipment 103 (therefore, the global IP address and WAN side port number of the router apparatus 104b) as a destination. Fig. 9 shows one example of the equipment information list stored in the table memory 101m included in the server apparatus 101.

The request acceptance equipment 103 periodically transmits the

equipment registration packet 201 to the server apparatus 101. Due to this, even if the global IP address or the WAN side port number of the router apparatus 104b is changed, the equipment information list on the server apparatus 101 is automatically updated by executing the step S202 and the step S202A similar to the step S202.

On the other hand, when the request issuance equipment 102 wishes to execute data communication with the request acceptance equipment 103, the first connection request sequence of the step S203 between the request issuance equipment 102 and the server apparatus 101, the step S204 by the server apparatus 101, the transmission of a packet 205, and a second connection request sequence of the step S206 between the server apparatus 101 and the request acceptance equipment 103 are executed as a series of processings so as to transmit a connection request message for notifying that the request issuance equipment 102 wishes to execute the data communication with the request acceptance equipment 103 from the request issuance equipment 102 to the request acceptance equipment 103. Then, the connection request message from the request issuance equipment 102 is relayed by the server apparatus 101 and transferred from the request issuance equipment 102 to the request acceptance equipment 103. The request issuance equipment 102 first of all executes a first connection request sequence of the step S203 between the request issuance equipment 102 and the server apparatus 101 so as to transmit the connection request message to the request acceptance equipment 103.

At the first connection request sequence of the step S203, it is

necessary to transmit secret information such as the password of the request acceptance equipment 103, the equipment ID of the request acceptance equipment 103, and the IP address and the port number as associated with the request issuance equipment 102. For this reason, SSL (Secure Socket Layer) is used to encrypt the secret information in the present preferred embodiment. An SSL communication used to encrypt transmission of the connection request packet 217, which will be described later, is first described with reference to Figs. 3 and 5.

Fig. 5 is a block diagram of a certificate authority apparatus 51 that authenticates whether or not the server apparatus 101 is valid for the request issuance equipment 102 and the request acceptance equipment 103. In particular, Fig. 5 shows a method of distributing server certificate data 65 for certifying validity of the server apparatus 101 and an authentication method. In Fig. 5, the router apparatuses 104a and 104b are not shown since they are not essential in the description relating to authentication. Referring to Fig. 5, the certificate authority apparatus 51 (where a certificate authority is referred to as a CA hereinafter) stores a pair of an inherent CA public key 52 and a CA secret key 53 in a table memory 51m of the certificate authority apparatus 51. The server apparatus 101 stores a pair of an inherent server secret key 61 and a server public key 62 as well as the server certificate data 65 issued by the certificate authority apparatus 51 in the table memory 101m of the server apparatus 101. The server certificate data 65 consists of the server public key 62 and a signature 64 generated by the certificate authority apparatus 51.

In order to execute the processings at the first connection request sequence of the step S203 and the second connection request sequence of the step S206, the server apparatus 101 needs first of all to cause the certificate authority apparatus 51 to issue the server certificate data 65 in advance according to processings described below.

The certificate authority apparatus 51 includes the table memory 51m that stores the pair of the CA public key 52 and the CA secret key 53 in advance. The server apparatus 101 generates the pair of the server public key 62 and the server secret key 61. The server apparatus 101 transmits the server public key 62 and information on the server apparatus 101 to the certificate authority apparatus 51 as a server certificate data request packet 63, and asks the certificate authority apparatus 51 to issue the server certificate data 65. When receiving the server certificate data request packet 63, the certificate authority apparatus 51 generates the signature 64 using the CA secret key 53 based on the information received from the server apparatus 101 and the other necessary information. Then, the certificate authority apparatus 51 issues data generated by combining the information received from the server apparatus 101, the other necessary information, and the signature 64 to the server apparatus 101 as the server certificate data 65. The server certificate data 65 thus issued is transmitted from the certificate authority apparatus 51 to the server apparatus 101 as a server certificate data issuance packet 54. The server apparatus 101 stores the received server certificate data 65 in the internal table memory 101m of the server apparatus 101.

The request issuance equipment 102 and the request acceptance equipment 103, serving as client equipments, acquire the CA public key 52 from the certificate authority apparatus 51 in advance, and store the acquired CA public key 52 in their respective internal memories 102m and 103m. In general, the CA public key 52 is distributed to the client equipments (that is, the other equipments which communicate with the server apparatus 101) in a form of the CA certificate data packet 55 combined with information on the certificate authority apparatus 51 and the like. When receiving the server certificate data 65 through a server certificate data packet 214 from the server apparatus 101, each of the request issuance equipment 102 and the request acceptance equipment 103 allows each of certificate information authentication processing sections 102c and 103c provided in respective equipments 102 and 103 to authenticate whether or not the signature 64 included in the server certificate data 65 is valid using the CA public key 52 stored in each of the internal table memories 102m and 103m. This leads to that each of the request issuance equipment 102 and the request acceptance equipment 103 can confirm whether or not the server public key 62 within the server certificate data 65 is valid.

Concretely, the step S203 of the first connection request sequence for a secret communication between the request issuance equipment 102 and the server apparatus 101 is executed as follows.

Fig. 3 is a sequence diagram showing detailed processings at the first connection request sequence of the step S203. Fig. 3 shows a flow for transmitting the connection request packet 217 using the SSL

communication. In Fig. 3, reference symbol 73 denotes a common key for communication used for the secret communication.

It is assumed that the server apparatus 101 further includes an encryption communication processing section 101e. The encryption communication processing section 101e generates common keys 73 and 83 for communication for encrypting and decoding signals to be transmitted and received, encrypts and decrypts the signals to be transmitted and received to and from the request issuance equipment 102 using the generated common key 73 for communication, and encrypts and decrypts the signals to be transmitted and received to and from the request acceptance equipment 103 using a common key 83 for communication. It is also assumed that the request issuance equipment 102 further includes an encryption communication processing section 102e and a certificate information authentication processing section 102c. The encryption communication processing section 102e of the equipment 102 generates the common key 73 for communication for encrypting and decrypting the signals to be transmitted and received, and executes encryption and decryption of the signals to be transmitted and received to and from the server apparatus 101 using the generated common key 73 for communication. The certificate information authentication processing section 102c authenticates whether or not the server certificate data 65 is valid.

In the SSL communication, the request issuance equipment 102 of a client side first of all transmits the TCP connection start packet 211 to the server apparatus 101 through the router apparatus 104a, and

this leads to that requesting that a communication with the server apparatus 101 be started by the TCP connection. Fig. 6 shows one example of the NAPT table stored in the internal table memory 104am of the router apparatus 104a. When the TCP connection start packet 211 passes through the router apparatus 104a, the router apparatus 104a translates the SA on the TCP connection start packet 211 from "192.168.1.11" to "4.17.168.2", and also translates the SP on the TCP connection start packet 211 from "1500" to "7000" using the NAPT function, according to the NAPT table. Further, when receiving the packet addressed to the request issuance equipment 102, the router apparatus 104a executes an opposite translation to the above translation to the DA on the packet and a different translation to the DP on the packet, and transmits the resulting packet to the request issuance equipment 102. In the present specification, the NAPT processing operation of the router apparatus 104a will not be described for brevity of description. However, actually, when the request issuance equipment 102 wishes to transmit or receive a packet to or from the server apparatus 101 or the other equipments on the Internet (WAN) 105, the equipment 102 always transmits and receives the packet through the router apparatus 104a, and the router apparatus 104a executes the NAPT processing to the packet.

Next, the request issuance equipment 102 and the server apparatus 101 execute encryption specification negotiation steps, thereby mutually checking encryption scheme specifications employed in the secret communication. The request issuance equipment 102 first

of all transmits an encryption communication start request packet (referred to as a client_hello packet) 212 to the server apparatus 101 using the TCP connection established by the TCP connection start packet 211. The encryption communication start request packet 212 includes an available SSL version, an available encryption scheme list, a session ID, and the like, and also includes a random number ClientHello. random generated by the request issuance equipment 102. When receiving the encryption communication start request packet 212 and permitting start of a communication, the server apparatus 101 transmits an encryption communication start response packet (referred to as "server hello packet") 213 to the request issuance equipment 102 using the TCP connection established by the TCP connection start packet 211. The encryption communication start response packet 213 includes an SSL version to be used (the latest version among those supported by both the request issuance equipment 102 and the server apparatus 101), a session ID, an encryption scheme to be used, and the like, and also includes a random number "ServerHello.random" generated by the server apparatus 101 in a manner similar to that of the random number "ClientHello.random". At the following first connection request sequence of the step S203, the SSL version and encryption scheme designated by the encryption communication start response packet 213 are used. The random numbers "ClientHellow.random" and "ServerHello.random" are generated by the request issuance equipment 102 and the server apparatus 101 independently of each other, as a 32-bit time stamp and a 28-byte

random number (or a sufficiently safe pseudo random number), respectively. The encryption communication start request packet 212 and the encryption communication start response packet 213 including the random numbers "ClientHellow.random" and "ServerHello.random", respectively, are transmitted without any encryption.

Then, the server apparatus 101 transmits a server certificate data packet 214 to the request issuance equipment 102. The transmission of the server certificate data packet 214 to the request issuance equipment 102 is not always after transmission of the encryption communication start response packet 213. As long as the server certificate data packet 214 is transmitted before reception of a common key generation information packet 215 for request-issuance equipment-side communication, which will be described later, the packet 214 may be transmitted at any timing (e.g., before the first connection request sequence of the step S203). The certificate information authentication processing section 102c of the request issuance equipment 102 confirms whether or not the server certificate data 65 included in the transmitted server certificate data packet 214 is valid using the CA public key 52 stored in the equipment 102, as already described above.

When confirming that the server certificate data 65 included in the transmitted server certificate data packet 214 is valid by the certificate information authentication processing section 102c, the request issuance equipment 102 starts a common key generation information exchange step including transmission and reception of common key generation information 71 for request-issuance

equipment-side communication and common key generation information 72 for server-apparatus-side communication.

At the common key generation information exchange step, the request issuance equipment 102 first of all generates the common key generation information 71 for request-issuance equipment-side communication by the encryption communication processing section 102e of the equipment 102. In addition, the request issuance equipment 102 transmits the common key generation information packet 215 for request-issuance equipment-side communication including this generated common key generation information 71 for request-issuance equipment-side communication, to the server apparatus 101 using the TCP connection established by the TCP connection start packet 211. The server apparatus 101 generates the common key generation information 72 for server-apparatus-side communication by the encryption communication processing section 101e of the apparatus 101 in response to the transmitted common key generation information packet 215 for request-issuance equipment-side communication. In addition, the server apparatus 101 transmits common key generation information packet 216 for server-apparatus-side communication including this generated common key generation information 72 for server-apparatus-side communication, to the request issuance equipment 102 using the TCP connection established by the TCP connection start packet 211. The request issuance equipment 102 and the server apparatus 101 generates the same common key 73 for communication by their encryption communication processing sections

102e and 101e based on the common key generation information 71 and 72, respectively. This leads to that it is possible to share the common key 73 for communication between the request issuance equipment 102 and the server apparatus 101.

A preferred embodiment of the common key generation information exchange changes according to the encryption scheme for use in SSL key exchange. When an RSA encryption scheme is used, the encryption communication processing section 102e of the request issuance equipment 102 generates, as the common key generation information 71 for request-issuance equipment-side communication, a 48-byte random number called "Pre Master Secret (PMS)", and encrypts the generated PMS using the server public key 62 included in the server certificate data 65. Then the request issuance equipment 102 transmits the encrypted PMS to the server apparatus 101 using the TCP connection established by the TCP connection start packet 211. The server apparatus 101 causes the encryption communication processing section 101e to decrypt the PMS that is received while being encrypted, using the server secret key 61 which the server apparatus 101 owns, thereby acquiring the transmitted PMS. Generation and transmission of the common key generation information 72 for server-apparatus-side communication are not performed. The server apparatus 101 and the request issuance equipment 102 generate the common key 73 for communication using the PMS, as will be described later, thereby sharing the key between them.

If a Diffie-Hellman encryption scheme is used, the request

issuance equipment 102 and the server apparatus 101 conclude an agreement about two parameters (i.e., a prime number "p" and a primitive root "g" of the prime number "p") for sharing a Diffie-Hellman key between them in advance. After receiving the server certificate data packet 214, the request issuance equipment 102 generates a random number "a", calculates a least positive remainder of g^a to modulus "p", as the common key generation information 71 for request-issuance equipment-side communication, and transmits the common key generation information packet 215 for request-issuance equipment-side communication including the common key generation information 71 for request-issuance equipment-side communication to the server apparatus 101. The server apparatus 101 generates a random number "b", calculates a least positive remainder of g^b to modulus "p", as the common key generation information 72 for server-apparatus-side communication, and transmits the common key generation information packet 216 for server-apparatus-side communication including the common key generation information 72 for server-apparatus-side communication to the request issuance equipment 102. Accordingly, the pieces of common key generation information thus mutually transmitted are used as the Diffie-Hellman public key. Furthermore, signatures of the request issuance equipment 102 and the server apparatus 101 may be added when the pieces of common key generation information 71 and 72 are transmitted, respectively.

If a fixed Diffie-Hellman encryption scheme of a kind of the Diffie-Hellman encryption scheme is used, the value included in the server

certificate data 65 is used as the information from the server apparatus 101. Therefore, the generation and transmission of the common key generation information 72 for server-apparatus-side communication are not performed.

As stated above, when the pieces of common key generation information 71 and 72 are exchanged between the request issuance equipment 102 and the server apparatus 101, the common key 73 for communication to be used as the secret key in a later communication is first generated using these pieces of common key generation information 71 and 72. In order to generate the common key 73 for communication, the PMS is generated based on the mutually exchanged common key generation information 71 and 72. In case of the RSA encryption scheme, the PMS is the common key generation information 71 for request-issuance equipment-side communication as described above. In case of the Diffie-Hellman encryption scheme, the PMS is generated using the Diffie-Hellman public keys of both the apparatus 101 and the equipment 102. In other words, the server apparatus 101 calculates the least positive remainder to modulus "p", which is a value obtained by multiplying the received least positive remainder of g^a to modulus "p" by a b^{th} power, as the PMS. The request issuance equipment 102 calculates the least positive remainder to modulus "p", which is a value obtained by multiplying the received least positive remainder of g^b to modulus "p" by an a^{th} power, as the PMS. If the Diffie-Hellman encryption scheme is used, the PMS calculated by each of the request issuance equipment 102 and the server apparatus 101 is

equal to the least positive remainder of g^{ab} to modulus "p".

In order to generate the common key 73 for communication from the PMS, the following calculation is conducted using two hash algorithms of MD5 (Message Digest 5) and SHA (Secret Hash Algorithm).

Common key master_secret =
MD5(PMS||SHA('A'||PMS||ClientHello.random
||ServerHello.random))||MD5(PMS||SHA('BB'||PMS
||ClientHello.random||ServerHello.random))||MD5(PMS||SHA('CCC'
||PMS||ClientHello.random||ServerHello.random)) (1)

In the Equation (1), "||" represents connection of bit sequences.

Thereafter, the request issuance equipment 102 and the server apparatus 101 encrypt and decrypt the connection request packet 217 using the common key "master_secret" calculated as expressed by the Equation (1) as the common key 73 for communication, and this leads to that the secret communication can be executed. In other words, when the sharing of the common key 73 for communication between the request issuance equipment 102 and the server apparatus 101 is completed, the request issuance equipment 102 causes the encryption communication section 102e of the equipment 102 to encrypt the data including the equipment ID of the connection target request acceptance equipment 103, the password of the request acceptance equipment 103, and the IP address and port number as associated with the request issuance equipment 102 and used for communication, using the

common key 73 for communication before transmission of the first connection request packet 217. It is noted that the IP address and port number as associated with the request issuance equipment 102 are the global IP address and WAN side port number of the request-issuance-side LAN 106a including the request issuance equipment 102, i.e., the WAN side global IP address and WAN side port number of the router apparatus 104a. The request issuance equipment 102 generates the connection request packet 217 with this encrypted data included as the payload, and transmits the generated connection request packet 217 to the server apparatus 101 using the TCP connection established by the TCP connection start packet 211. More specifically, the request issuance equipment 102 transmits the connection request packet 217 shown in Fig. 7C to the router apparatus 104a. In addition, the router apparatus 104a executes the NAPT processing to the received connection request packet 217, and transmits the connection request packet 217, shown in Fig. 7D, which has been subjected to the NAPT processing, to the server apparatus 101. On the other hand, the server apparatus 101 receives the connection request packet 217 including the encrypted data as the secret information from the request issuance equipment 102 using the TCP connection established between the server apparatus 101 and the request issuance equipment 102. In response to the reception of the packet 217, the server apparatus 101 causes the encryption communication processing section 101e of the server apparatus 101 to decrypt the encrypted data using the common key 73 for communication.

The WAN side global IP address and WAN side port number of the router apparatus 104a written in the connection request packet 217 are used when the TCP connection start packet 208 and a packet as associated with a data communication sequence of the step S209, which will be described later, are transmitted and received. In other words, the request issuance equipment 102 receives the TCP connection start packet 208 from the request acceptance equipment 103, and establishes the TCP connection between the equipments 102 and 103. When the request issuance equipment 102 transmits and receives the packet as associated with the data communication sequence of the step S209 (as described later) using the established TCP connection, the WAN side global IP address and WAN side port number of the router apparatus 104a are written into the packet thus transmitted and received. It is assumed that the WAN side global IP address and WAN side port number of the router apparatus 104a written into the packet can be translated to the private IP address and port number of the request issuance equipment 102 using the NAPT function of the router apparatus 104a or vice versa.

If the port number based on which the request issuance equipment 102 receives the TCP connection start packet 208 from the request acceptance equipment 103 is, for example, "1600", the NAPT table of the router apparatus 104a is that shown in Fig. 6.

A second row of the NAPT table shown in Fig. 6 is a translation table used when the request issuance equipment 102 receives the TCP connection start packet 208 from the request acceptance equipment

103 and the packet at the later data communication sequence of the step S209. The request acceptance equipment 103 transmits the TCP connection start packet 208 to the router apparatus 104a that has the global IP address of "4.17.168.2" and the port number of "5000" so as to establish the TCP connection. Then, the IP address and the port number written in the TCP connection start packet 208 are translated to the private IP address of the request issuance equipment 102 and the port number of the router apparatus 104a, respectively, by the NAPT function of the router apparatus 104a. Finally, the request acceptance equipment 103 can establish the TCP connection with the request issuance equipment 102.

When receiving the connection request packet 217, the server apparatus 101 makes reference to a plurality of sets of equipment information in the equipment information list, shown in Fig. 9, stored in the internal table memory 101m of the server apparatus 101, and searches the equipment ID of "2133" of the request acceptance equipment 103 included in the received connection request packet 217 from the equipment information list at step S204. If finding out the equipment ID coincident with "2133" on the equipment information list, the server apparatus 101 identifies the equipment related to a set of equipment information including this equipment ID of "2133" as the connection target request acceptance equipment 103. In addition, the server apparatus 101 identifies the IP address and the port number included in a set of equipment information on the identified request acceptance equipment 103 as the IP address and port number as

associated with the request acceptance equipment 103, respectively. The server apparatus 101 does not promptly transmit the IP address and port number and the password of the request acceptance equipment 103 included in the received connection request packet 217 and associated with the request issuance equipment 102, to the request acceptance equipment 103. In this case, the server apparatus 101 transmits the connection request notification packet 205 using the UDP, with an IP address of "202.204.16.13" and a port number of "3400" as associated with the request acceptance equipment 103 (included in the same set of equipment information as an equipment ID of "2133") as a destination. The connection request notification packet 205 is transmitted to the router apparatus 104b as the response signal to the equipment registration packet 201. The router apparatus 104b performs the translation of the IP address and the port number, and the packet 205 including the translated IP address and port number can, therefore, arrive at the request acceptance equipment 103. As shown in Figs. 8A and 8B, the connection request notification packet 205 includes a connection request notification flag showing that the packet indicates a connection request notification.

When receiving the connection request notification packet 205, the request acceptance equipment 103 executes the second connection request sequence of the step S206 between the request acceptance equipment 103 and the server apparatus 101.

Fig. 4 is a sequence diagram showing detailed processings at the second connection request sequence of the step S206. At the second

connection request sequence of the step S206, in a manner similar to that of the first connection request sequence of the step S203, it is necessary to transmit secret information such as the password of the request acceptance equipment 103 and the IP address and port number as associated with the request issuance equipment 102. For this reason, the SSL is used to encrypt the secret information in the present preferred embodiment. It is assumed that the request acceptance equipment 103 further includes an encryption communication processing section 103e and a certificate information authentication processing section 103c. The encryption communication processing section 103e of the equipment 103 generates the common key 83 for communication for encrypting and decrypting the signals to be transmitted and received, and executes encryption and decryption of the signals transmitted and received to and from the server apparatus 101 using the generated common key 83 for communication. The certificate information authentication processing section 103c of the equipment 103 authenticates whether or not the server certificate data 65 is valid. The second connection request sequence of the step S206 for the secret communication between the server apparatus 101 and the request acceptance equipment 103 is executed as follows.

In the SSL communication, the request acceptance equipment 103 of a client side first of all transmits a TCP connection start packet 221 to the server apparatus 101 through the router apparatus 104b, thereby requesting that a communication with the server apparatus 101 be started by the TCP connection. When the TCP connection start

packet 221 passes through the router apparatus 104b, the router apparatus 104b translates the SA and the SP on the TCP connection start packet 221 using the NAPT function used when the equipment registration packet 201 is transmitted. Further, when receiving the packet addressed to the request acceptance equipment 103, the router apparatus 104b executes an opposite translation to the DA on the packet to the translation performed on the SA and a different translation to the DP on the packet from the translation performed on the SD, and then, transmits the resultant packet to the request acceptance equipment 103. In the present specification, the NAPT processing operation of the router apparatus 104b will not be described for brevity of description. However, actually, when the request acceptance equipment 103 wishes to transmit or receive a packet, the equipment 103 always transmits or receives the packet through the router apparatus 104b, and the router apparatus 104b executes the NAPT processing to the packet.

Next, the request acceptance equipment 103 and the server apparatus 101 executes encryption specification negotiation steps, thereby mutually checking encryption scheme specifications employed in the secret communication. The request acceptance equipment 103 first of all transmits an encryption communication start request packet (referred to as "client_hello packet") 222 to the server apparatus 101 using the TCP connection established by the TCP connection start packet 221. The encryption communication start request packet 222 includes an available SSL version, an available encryption scheme list,

a session ID, and the like, and also includes a random number ClientHello. random generated by the request acceptance equipment 103. When receiving the encryption communication start request packet 222 from the request acceptance equipment 103, the server apparatus 101 transmits an encryption communication start response packet (referred to as "server_hello packet") 223 to the request acceptance equipment 103 using the TCP connection established by the TCP connection start packet 221. The encryption communication start response packet 223 includes an SSL version to be used (the latest version among those supported by both the request issuance equipment 102 and the server apparatus 101), a session ID, an encryption scheme to be used, and the like, and also includes a random number "ServerHello.random" generated by the server apparatus 101. At the following second connection request sequence of the step S206, the SSL version and encryption scheme designated by the encryption communication start response packet 223 are used. The random numbers "ClientHellow.random" and "ServerHello.random" are generated by the request acceptance equipment 103 and the server apparatus 101 independently of each other, as a 32-bit time stamp and a 28-byte random number (or a sufficiently safe pseudo random number), respectively. The encryption communication start request packet 222 and the encryption communication start response packet 223 including the random numbers "ClientHellow.random" and "ServerHello.random", respectively, are transmitted without any encryption.

Then the server apparatus 101 transmits the server certificate data packet 214 to the request acceptance equipment 103. The transmission of the server certificate data packet 214 to the request acceptance equipment 103 is not always after transmission of the encryption communication start response packet 223. As long as the server certificate data packet 214 is transmitted before reception of a common key generation information packet 224 for request-acceptance equipment-side communication, the packet 214 may be transmitted at any timing (e.g., before the second connection request sequence of the step S206). The certificate information authentication processing section 103c of the request acceptance equipment 103 confirms whether or not the server certificate data 65 included in the transmitted server certificate data packet 214 is valid using the CA public key 52 stored in the equipment 103, in a manner similar to that of the instance of the request issuance equipment 102 described above with reference to Fig. 5.

When confirming that the transmitted server certificate data 65 included is valid by the certificate information authentication processing section 103c, the request acceptance equipment 103 starts a common key generation information exchange step including transmission and reception of common key generation information 81 for request-acceptance equipment-side communication and common key generation information 82 for server-apparatus-side communication.

At the common key generation information exchange step, the request acceptance equipment 103 first of all generates the common

key generation information 81 for request-acceptance equipment-side communication by the encryption communication processing section 103e of the equipment 103. In addition, the request acceptance equipment 103 transmits the common key generation information packet 224 for request-acceptance equipment-side communication including this generated common key generation information 81 for request-acceptance equipment-side communication, to the server apparatus 101 using the TCP connection established by the TCP connection start packet 221. The server apparatus 101 generates the common key generation information 82 for server-apparatus-side communication by the encryption communication processing section 101e of the server apparatus 101 in response to the transmitted common key generation information packet 224 for request-acceptance equipment-side communication. In addition, the server apparatus 101 transmits a common key generation information packet 225 for server-apparatus-side communication including this generated common key generation information 82 for server-apparatus-side communication, to the request issuance equipment 102 using the TCP connection established by the TCP connection start packet 221. The request issuance equipment 102 and the server apparatus 101 generates the same common key 83 for communication by their encryption communication processing sections 102e and 101e based on the common key generation information 81 and 82, respectively. In order to generate the common key 83 for communication, the RSA encryption scheme, the Diffie-Hellman encryption scheme, or the like is used in a

manner similar to that of the first connection request sequence of the step S203. The generated pieces of common key generation information 81 and 82 are exchanged between the request acceptance equipment 103 and the server apparatus 101, respectively. The encryption communication processing sections 103e and 101e of the request acceptance equipment 103 and the server apparatus 101 generate the common keys 83 for communication to be used as the secret key for a later communication by using these pieces of common key generation information 81 and 82, respectively.

Then, it is possible to share the common key 83 for communication between the request acceptance equipment 103 and the server apparatus 101. The server apparatus 101 and the request acceptance equipment 103 encrypt and decrypt the connection request packet 226 using the common key 83 for communication, and this leads to that a secret communication can be executed between them. In other words, after reception of the first connection request packet 217 and before transmission of the second connection request packet 226, when the sharing of the common key 83 for communication between the request acceptance equipment 103 and the server apparatus 101 is completed, the server apparatus 101 causes the encryption communication processing section 101e of the apparatus 101 to encrypt the data including the password of the request acceptance equipment 103 included in the connection request packet 217, and the global IP address of "4.17.168.2" and port number "5000" of the router apparatus 104a to be used for communication, using the

common key 83 for communication. The server apparatus 101 generates the connection request packet 226 with this encrypted data included as the payload, and transmits the generated connection request packet 226 to the request acceptance equipment 103 using the TCP connection established by the TCP connection start packet 221 as a response signal to the equipment registration packet 201. More specifically, the server apparatus 101 transmits the connection request packet 226 shown in Fig. 8D to the router apparatus 104b, using the IP address and port number identified as those of the request acceptance equipment 103 in the equipment information list of the server apparatus 101 at step S204 shown in Fig. 2 as a destination. In addition, the router apparatus 104b executes the NAPT processing to the received connection request packet 226, and transmits the connection request packet 226, shown in Fig. 8C, which has been subjected to the NAPT processing, to the request acceptance equipment 103. On the other hand, the request acceptance equipment 103 receives the connection request packet 226 including the encrypted data as the secret information from the server apparatus 101 using the TCP connection established between the server apparatus 101 and the request acceptance equipment 103. In response to the reception of the packet 226, the request acceptance equipment 103 causes the encryption communication processing section 103e of the equipment 103 to decrypt the encrypted data using the common key 83 for communication. In this way, the connection request message for notifying that the request issuance equipment 102 desires to execute

the data communication with the request acceptance equipment 103 is eventually transmitted from the request issuance equipment 102 to the request acceptance equipment 103.

Referring again to Fig. 2, the request acceptance equipment 103 authenticates whether or not the password included in the connection request packet 226 coincides with the password of the request acceptance equipment 103 stored in the internal table memory 103m of the request acceptance equipment 103, and therefore, is valid at step S207. Only when the password is valid, the request acceptance equipment 103 transmits the TCP connection start packet 208 to the router apparatus 104a as a communication request signal for requesting that a communication between the request issuance equipment 102 and the request acceptance equipment 103 be started by the TCP connection to the request issuance equipment 102 as associated with the IP address of "4.17.168.2" and port number of "5000" included in the connection request packet 226. The TCP connection start packet 208 arrives at the request issuance equipment 102 by the NAPT function of the router apparatus 104a as stated above. The request acceptance equipment 103 can thus establish the TCP connection with the request issuance equipment 102.

After the request issuance equipment 102 accepts the communication between the request issuance equipment 102 and the request acceptance equipment 103 in response to the TCP connection start packet 208, the request issuance equipment 102 and the request acceptance equipment 103 can execute the data communication

sequence of the step S209 using the TCP connection established by the TCP connection start packet 208.

In this way, by using the server apparatus 101, the data communication can be executed between the request issuance equipment 102 and the request acceptance equipment 103 each having the private IP address and located on the different LAN's of the LAN 106a and the LAN 106b, respectively.

Even if the request issuance equipment 102 owns the global IP address and is directly connected to the Internet (WAN) 105, the communication can be executed between the request issuance equipment 102 and the request acceptance equipment 103 through the same operation as that stated above. Further, even if the request acceptance equipment 103 owns the global IP address and is directly connected to the Internet (WAN) 105, the communication can be executed between the request issuance equipment 102 and the request acceptance equipment 103 through the same operation as that stated above. In either case, the same operation as that stated above are carried out except that the router apparatus does not perform the translation of the IP address and the port number.

In the present preferred embodiment, the server apparatus 101, the request issuance equipment 102, and the request acceptance equipment 103 are connected to the Internet (WAN) 105. However, the present preferred embodiment is not limited to this. The server apparatus 101, the request issuance equipment 102, and the request acceptance equipment 103 may be constituted to be connected to one of

or both of the other open network and a dedicated network.

In addition, even if each of the router apparatuses 104a and 104b includes not the NAPT function but the NAT function only, the communication can be executed between the request issuance equipment 102 and the request acceptance equipment 103 by the same operation as that stated above. In this case, each of the router apparatuses 104a and 104b does not perform the translation of the port number.

The request issuance equipment 102 may always keep a combination of the IP address and the port number for receiving the TCP connection start packet 208 as that set in the NAPT table shown in Fig. 6, or may set this combination in the NAPT table when transmitting the TCP connection start packet 211 at the first connection request sequence of the step S203 and delete this combination from the NAPT table when finishing the data communication sequence of the step S209. The setting of the NAPT table may be made using either the static NAPT or a function such as universal plug and play.

Furthermore, the communication through the TCP connection started by the TCP connection start packet 211 at the first connection request sequence of the step S203 and the communication through the TCP connection started by a TCP connection start packet 221 at the second connection request sequence of the step S203 may be established using an encryption communication scheme different from the SSL. Alternatively, the TCP communication encryption at steps S203 and S206 may be omitted. In the latter case, at step S203, the

request issuance equipment 102 may transmit the connection request packet 217 soon after transmitting the TCP connection start packet 211 to thereby establish the TCP connection. At step S206, the server apparatus 101 may transmit the connection request packet 226 soon after receiving the TCP connection start packet 221.

The processings at the data communication sequence of the step S209 may be executed using the encryption connection scheme such as the SSL scheme similarly to the steps S202 and S206. In addition, the data transmission and reception at step S209 may be executed using the other transmission protocol such as the UDP.

The equipment registration packet 201, the connection request packet 217, the connection request notification packet 205, and the connection request packet 226 shown in Figs. 7A to 7D and 8A to 8D are given only for illustrative purposes. The other field may be additionally used or the respective fields may be provided in a different order.

The IP addresses, the port numbers, and the equipment IDs employed in Figs. 1 to 9 are given only for illustrative purposes. They may be different values.

As another preferred embodiment, the present invention may be provided as a computer readable program including the respective steps in the processings shown in Figs. 2 to 4. Alternatively, the present invention may be provided as a computer readable recording medium that records this program. In the latter case, the program is read out by a computer or an equipment connected to the Internet, and the steps

included in the program are executed by the computer or the equipment. Then, the computer or the equipment can operate as all of or one of the server apparatus 101, the request issuance equipment 102, and the request acceptance equipment 103 according to the preferred embodiment stated before. Examples of the recording medium that records the program may include optical recording mediums such as a CD-ROM and a DVD-ROM, magnetic recording mediums such as a flexible disk and a hard disk, and a semiconductor memory. However, the type of the recording medium that records the program is not limited to them. In addition, the program may be distributed through the network such as the Internet.

As described above, the present invention can provide the communication system capable of easily realizing a pier to pier communication between equipments connected to the Internet (WAN) and positioned on different LANs and prohibiting an illegal access.

INDUSTRIAL APPLICABILITY

Accordingly, as mentioned above in detail, according to the present invention, there can be realized a pier to pier communication between the request issuance equipment and the request acceptance equipment which are equipments each having a private IP address but located on different LANs with prohibiting any illegal access. Further, according to the present invention, the program can be provided including the steps in the communication method for allowing a computer or an equipment connected to the Internet to execute the steps in the communication method when the program is read out by

the computer or the equipment.